Amendments to the Specification:

Please replace paragraph 42 on page 9 of the specification with the following rewritten paragraph.

[0042] FIG. 3 illustrates an embodiment of distributed filtering consistent with the principles of the invention. An attack from one or more malicious users is initially detected at the firewall. The firewall includes attack detection elements, and responds to the attack by creating attack information and sending the attack information to routers B, C, and D in control packets, as indicated by broken line arrows in FIG. 3. Note that the source address used by the attacking systems might be legitimate, or might be made up. If the network has the ability to check the correctness of source addresses at all input points, then the source address of the attacking packets will be legitimate, and the firewall can determine where the attack is coming from, and the notification may be ~~send~~ sent to only the ingress routers from which the attack is arriving at the network. If the network does not have the ability to check source addresses at all ingress points, then initially, when the firewall detects the attack, it is not known where the attack is coming from. In this case the message describing the attack may be sent to all ingress routers (such as routers A, B, and C in figure 3). If the attack packets are well distinguished from other packets, or if stopping the attack completely is important enough to justify dropping other packets as well, then the ingress routers may be told to discard all packets which match the description of the attacking packets. Otherwise, the ingress routers may be told to rate limit all packets which match the description of the attack packets. Also note that the ingress routers may

also be told to count packets which match the description of the attack packets, which facilitates later analysis of the form and location of the attack.